ABSTRACT

A port profiling system detects unauthorized network usage. The port profiling system analyzes network communications to determine the service ports being used. The system collects flow data from packet headers between two hosts or Internet Protocol (IP) addresses. The collected flow data is analyzed to determine the associated network service provided. A host data structure is maintained containing a profile of the network services normally associated with the host. If the observed network service is not one of the normal network services performed as defined by the port profile for that host, an alarm signal is generated and action can be taken based upon the detection of an Out of Profile network service. An Out of Profile operation can indicate the operation of a Trojan Horse program on the host, or the existence of a non-approved network application that has been installed.